ADDENDUM

Technical and Organizational Measures in accordance with Article 32 GDPR

Organization:

Hostway Deutschland GmbH
Am Mittelfelde 29
D-30519 Hannover
Germany
- Henceforth HWD -

As represented by the directors:
Dr. Achilleas Anastasiadis, Cord Bansemer, and Ilja Kassühlke

As of May 2, 2018

Preamble

HWD may, within the scope of the provision of services, come into contact with personal data. The processing of personal data, however, does not lie at the focus of the actual service provision of HWD. However, it cannot be ruled out, that within the scope of the provided services, technical access to the customers' personal may become possible by HWD. According to Article 32 GDPR, HWD shall implement appropriate technical and organizational measures, whenever personal data is processed. These measures are required to demonstrate compliance with the provisions of the data privacy laws.

HWD meets these requirements by the following measures:

1. Confidentiality according to Article 32 (1) (b) GDPR

a. Physical Access Control

Physical access to the main entrance of the HWD building as well as to all side entrances is restricted by a fence. The doors and gates of the fenced area are closed by default and can only be opened by HWD staff on site with transponders. Additionally, the main gate and the main entrance of the fenced area can be opened by HWD Network Operation Center (NOC) staff via doorbell and connected manual opening function.

All access paths to the building entrances of HWD are protected by video surveillance. The NOC staff have a 24/7 live visual display of all camera footage on screens in the NOC dedicated to that purpose.

Access ways to the building are by default closed and can only be opened from the outside with security keys. Building access is monitored around the clock by qualified staff on the central reception desk/ NOC, and each staff, customer, or supplier has to register at the central reception desk. Upon registering, visitors receive a visitor pass, which must be returned upon leaving the building. Visitors are instructed about the house rules upon visiting. Visitors have to either have the authorization to register themselves, or otherwise be authorized by persons with the appropriate authorization level to authorize others for registration. The identity of visitors has to be confirmed with a valid photo identification card. Visitors are personally escorted by staff into the building from the reception area. Organizational procedures and rules ensure that strangers should never stay or move within the building unattended.

Access to the data center footprint is protected by an access control system and unaccompanied access only possible for HWD staff. For the data center “Am Mittelfelde 29” this access control has been implemented with 2-factor-authentication. Access is logged. Access logs and video footage is checked daily by HWD staff.

Outside business hours the premises are controlled by an alarm system according to VDE standard. System alerts are monitored by a security service, and a documented intervention plan is followed. Additionally, all technical premises, access paths, as well as the perimeter defense, are video surveilled. Notably, all data center footprint is video surveilled, which is additionally supported by motion sensors.

b. Logical Access Control

No unauthorized access to data processing systems is granted. Access to our electronic data processing systems through external interfaces is firewall protected. Sensitive services, which must not be accessible publicly, are protected through a VPN. Publicly accessible systems, such as email and internet access are isolated from other services through appropriate segmentation. HWD operates diverse, depending on the security classification, in part physically separated networks. All systems are password-protected and only allow user-specific access. Group access is not implemented. In addition to strong password requirements on the basis of internal password guidelines, a 2-factor-authentication system is used for authentication on sensitive systems of HWD. HWD’s password policy, besides defining password complexity requirements, also includes additional framework parameters, such as the mandatory password resetting within defined terms, as well as prohibiting reuse of the same password.

Access privileges to customer equipment are handled in detail according to specific customer instruction and based on the services provided by HWD. According to HWD internal policies, depending on system type and classification, failed login attempts are responded to in different appropriate manners. Along with temporary access blocking, dynamic addition of network blocking, or permanent access removal, also logging and alerting takes place.

c. Data Access Control

Access to network directories or systems on which personal data is stored is limited to persons directly associated with the implementation of services, for which these data shall be used. Each user has to authenticate themselves with personalized access data. Initial access is limited to the internal HWD network, whenever system functions and customer instructions allow. In the case of external login (VPN) into the internal network of HWD, the staff receives access to network segments relevant to his duties. In the case of external access, additionally, 2-factor-authentication is deployed. For access to customer systems and equipment, customer-specific measures are agreed on with the customer. General access paths for HWD employee access on customer systems, if pertinent to the assignment, are protected with strong encryption.

HWD staff is only granted necessary privileges, as defined for the system or application. There is a clear distinction between administrators of an application or system and additional user groups. Access privileges are checked bi-annually with regards to need and correct configuration in the context of the internal auditing process.

d. Separation Control

HWD processes proprietary personal data only within the scope of systems and processes needed for the specific assignment. Within the scope of proprietary processing of personal data, HWD separates test environments from production environments. Depending on the service provided, HWD segregates customer data either physically (separate hardware systems, e.g. “dedicated server hosting”), or logically. Logical segregation may be realized in different ways, depending on the service provided. (“virtual server,” “multitenant software”).
The customer is responsible for any further separation control measures for the storage and processing of personal data within the scope of the order processing.

2. Integrity according to Article 32 (1) (b) GDPR

a. Data Transfer Control

The transmission of personal or other confidential data occurs with transport encryption or higher. HWD has an internal policy concerning the use of cryptographic methods, with clear definitions about which cryptographic methods are permissible in which constellation and with which technical specifications. HWD thereby follows the guidelines of the German Federal Office for Information Security (BSI), as well as those of the US National Institute of Standards and Technology (NIST).

Furthermore, HWD recommends the use of file-based encryption for the customer communication, whenever personal data is transferred. This way, even the temporary storage of data on HWD or the customer side is secured. This method requires, however, that the customer has the technical capacity to receive or transmit such an encrypted file. Insofar as HWD identifies this possibility with the customer, HWD will use such a method of file-based encryption, in coordination with the customer.

HWD follows a standard process for the storage, deletion, and physical destruction of data media. The data media, their safe storage location, as well as their consecutive return, deletion, or destruction, are logged accordingly. The destruction security level is H-4 according to the DIN standard 66399-2.

The shipping of personal data follows the strict conditions and safeguards provided for by law. Mobile data media with personal data are only stored in secured premises, and, if not in use, in a safe. Data which are no longer required for the provisioning of an order, e.g., blocked data, are stored in a separate, access-protected storage area. The repair and disposal of data media or hardware occur only by appropriately liable and certified companies. The same holds true for the disposal of data on paper.

b. Data Entry Control

Only selected staff may access the customer systems and data within the scope of a customer project. Thereby, only staff are selected, who are needed for the provisioning of the contractually agreed upon services. The legitimation of staff follows from the allocation to the group of staff, assigned for a particular customer. All staff has been committed to maintaining confidentiality, as well as to comply with legal requirements and internal policies.

Activities on customer systems are logged. Where technically possible, all changes and actions are automatically logged. Additionally, manual logging of activity is recorded and periodically inspected on a random basis.

The default operating instruction to staff is, not to modify or manipulate any personal data of the customer. Only at the explicit instruction of the customer any personal data on the customer systems may be modified. Exceptions are made for control processes for the administration of data (data backup, deletion of log data after a contractually agreed upon retention period, etc.), which occur within the scope of the operation of customer instances in default log files of the deployed server software, and which may also include personal data.

3. Availability and Resilience according to Article 32 (1) (b) GDPR

a. Availability Control

HWD operates two physically independent, and spatially separated data centers. The safeguarding of the availability of customer specific data is regulated in the agreement terms concerning the service level and service availability. HWD operates data backup storage in both data centers to this end, in order provide the possibility for cross-section data backup. Backup intervals are individually designed in agreement with the customer. For HWD's IT systems and data which are also required for the operation of the data center and therefore the availability of customer systems and data, a daily cross-section backup takes place, as well as an additional backup of all modified data, after the completion of works on HWD systems. Furthermore, storage systems, on which customer systems are operated, are protected from data loss using fault-tolerant RAID systems. Depending on the individual configuration agreement, however, there might be customer specific differences. The customer is responsible for electronic data processing systems which have been either rented by a third-party or are proprietary customer systems, which are collocated with HWD. A fire detection system is in use to minimize potential fire damage. A security company monitors alerts and follows a documented intervention plan in the case of an alert.

There are N+1 air conditioning units operational, and an emergency generator backs them.
Both data center locations have UPS systems, as well as an emergency power generator.

HWD performs active emergency prevention management within the scope of an active information security management system according to ISO-27001 on the basis of IT-Grundschutz. This ISMS includes, along with the continuous development of the emergency manual, the periodic performance of emergency testing. These tests occur at least bi-annually in the form of detailed simulation games. At least once a year, additionally, a so-called „black building test" is performed, to simulate a complete power outage. The performance of these exercises, as well as the findings, are recorded.

HWD monitors the availability of all systems required for the data center operation. Additionally, HWD monitors by default also the availability of customer systems. The monitoring scope for customer systems is determined by the customer during the provisioning phase and may be adjusted during the business relationship. As well as a timely alert in case of outage or malfunction of relevant systems or application, HWD can also provide evidence for the availability of a system or an application.

4. Process for regular Testing, Assessment, and Evaluation (Article 32 (1) (d); Article 25 (1) GDPR)

a. Data Protection Management

HWD operates a data protection management system. To this end, HWD has appointed a data protection officer, who maintains the data protection management system and reports directly to the management. Within the scope of the data protection management system HWD logs all procedures and actions that involve the processing of personal data in internal company procedure directories. Likewise, HWD operates an ISMS according to ISO-27001 on the basis of IT-Grundschutz and has been certified by the (German) Federal Office for Information Security (BSI) according to this standard. The certificate is re-assessed on an annual basis, and every three years a new application has to be submitted and a full audit performed. Technical organizational measures are audited on an annual basis, also within the annual certificate surveillance audit.

Within the framework of the data protection management system, HWD makes data protection impact assessments, if the need is identified. Additionally, HWD ensures, that all staff commit to compliance with confidentiality and data protection laws in writings, and renew their commitment annually. Likewise, a periodic awareness-raising and training process of all staff has been established.

b. Incident Response Management

HWD maintains within the framework of the established ISMS a documented process for incident response management. Together with escalation and reporting channels, this process also includes review and analysis, and consecutive optimization based on gained insights.

HWD deploys, both, equipment-based, as well as network-based solutions (intrusion detection, virus, and malware detection, anti-spam filters, as well as anomaly detectors) for the detection of incidents. HWD also monitors the infrastructure and customer systems with a monitoring solution with regards to outages and anomalies.

All incidents are documented in a ticketing system within the framework of the incident response management system. Both, the data protection officer (if personal data is involved), and the IT security must be included in the escalation process.

c. Data Protection by Default (Article 25 (2) GDPR)

HWD follows the principle of data minimization. Only data necessary for the specific process/context are processed and stored. The data protection officer regularly checks the appropriateness. All privileges are assigned according to the “need-to-have”-principle and must be justified. The assignment of privileges is regularly checked and questioned during the internal review process.

Storage and deletion terms are actively defined. The data protection officer monitors their observance.

d. Order Control (Outsourcing to Third-Parties)

HWD assesses (sub-) contractors within the framework of the supplier selection process, as well as during the continuous cooperation with regards to appropriate data protection and IT security processes. To this end, HWD performs a due diligence examination during the selection process of a (sub-) contractor, as well as random checks (documentation and on-site).

HWD ensures that all (sub-) contractors have contractually committed themselves to compliance with existing confidentiality obligations, as well as with data protection requirements. To this end, HWD enters a contractual agreement with regards to the handling of personal data with all (sub-) contractors.

Hostway Deutschland GmbH

- The Management -